MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

TIA2221 – INFORMATION ASSURANCE AND SECURITY

(All Sections / Groups)

2nd MARCH 2016
2.30 p.m. - 4.30 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 printed pages including cover page with 10 MCQ questions in Section A and 5 questions in SECTION B.

2. Attempt **ALL** questions in Section A and attempt **FOUR** out of **FIVE** questions in Section B. Marks and the distribution of marks for each question is given.

3. Please write all your answer in the Answer Booklet provided.

Section A: Attempt ALL questions. [10 Marks]

1. If risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets" the risk has all of the following elements **EXCEPT**?
A. An impact of assets based on threats and vulnerabilities.
B. Controls addressing the threats.
C. Threats to and vulnerabilities of processes and/or assets.
D. Probabilities of the threats.

2. Which choice below is an accurate statement about standards?
A.Standards are the high-level statements made by senior management in support of information systems security.
B.Standards are the first element created in an effective security policy program.
C.Standards are used to describe how policies will be implemented within an organization.
D.Standards are senior management's directives to create a computer security program.

3. Which is the best defense against network sniffing?
A. Use of switches (over hubs)
B. Use of wired networks (not wireless)
C. Use of gateway
D. Encryption

4. A timely cancellation of system access records would be an example of which basic security function?
A. Avoidance
B. Deterrence
C. Prevention
D. Detection

5. When an organization is determining which data is sensitive, it must consider all of the following **EXCEPT**:
A. Expectations of customers
B. Legislation or regulations
C. Quantity of data
D. Age of the data

6. Which choice below most accurately describes the organization's responsibilities during an unfriendly termination?
A. System access should be removed as quickly as possible after termination.
B. The employee should be given time to remove whatever files he needs from the network.
C. Cryptographic keys can remain the employee's property.
D. Physical removal from the offices would never be necessary.

Continued ...

7. Recovery controls attempt to:
A. Establish countermeasures to prevent further incidents
B. Return to normal operations
C. Compensate for vulnerabilities in other systems
D. Ensure that audit logs are reviewed regularly

8. A business continuity plan (BCP) should have a structure that includes:
A. A detailed section on incident and risk assessment covering all the organization's key business activities.
B. A detailed section on incident and risk assessment covering all the organization's business activities.
C. A brief section on incident and risk assessment covering all the organization's key business activities.
D. A brief section on incident and risk assessment covering all the organization's business activities.

9. A business impact analysis would **NOT** likely include which of the following tasks?
A. Calculating risk
B. Identifying threats
C. Selecting team members
D. Identifying critical functions of the company

10. Why is computer crime difficult to investigate:
A. Privacy laws protect people from being investigated.
B. Computer crime investigations require special techniques and tools.
C. Criminals can spoof their address.
D. The police have no jurisdiction over the Internet.

Continued ...

Section B: Attempt FOUR out of FIVE questions.

Question 1 [10 Marks]

(a) Give **THREE** reasons why greater attention should be directed at the vulnerability black market issue? [3 Marks]

(b) Describe any **FOUR** steps on how we could protect our data and minimize damage from hacking for general computer system? [4 Marks]

(c) How workforce analytics can help to prevent insider threat? [3 Marks]

Question 2 [10 Marks]

(a) Describe the weaknesses of passive networking scanning. [3 Marks]

(b) State **THREE** advantages of host-based assessment. [3 Marks]

(c) Why separation of duties is important among staff in an organisation? [2 Marks]

(d) Define "Outsider Threat". [2 Marks]

Question 3 [10 Marks]

(a) Describe both advantages and disadvantages involving law enforcement in Incident Detection. [4 Marks]

(b) Define "Incident Classification". [3 Marks]

(c) What is the main goal of Contingency Planning? [3 Marks]

Question 4 [10 Marks]

(a) Describe how Local Security Authority Subsystem Service (LSASS) helps to protect servers? [3 Marks]

(b) What is Identity Theft? Give **THREE** examples. [4 Marks]

(c) Provide any **THREE** counts of Incident Management Metrics. [3 Marks]

Continued ...

Question 5 [10 Marks]

(a) Explain Incident Response Team functions. [3 Marks]

(b) State **FIVE** steps taken by Trusted Program when consuming content. [5 Marks]

(c) Briefly explain Digital Right Management. [2 Marks]

End of Page